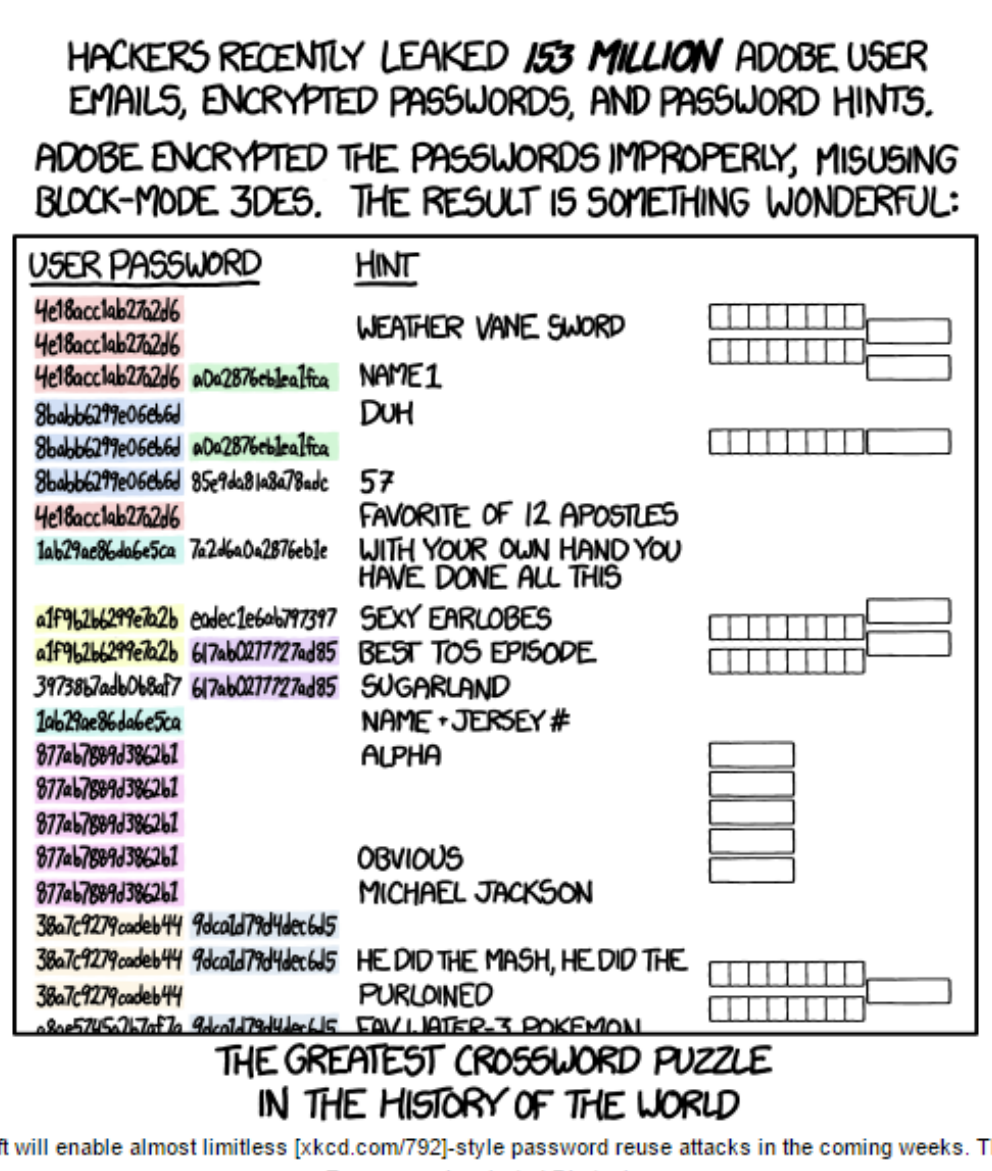
It seems you are using noscript, which is stopping our project wonderful ads from working. Explain xkcd uses ads to pay for bandwidth, and we manually approve all our advertisers, and our ads are restricted to unobtrusive images and slow animated GIFs. If you found this site helpful, please consider whitelisting us.

Want to advertise with us, or donate to us with Paypal or Bitcoin?

# 1286: Encryptic

|< < Prev Comic #1286 (November 4, 2013) Next > >|

## Encryptic


HACKERS RECENTLY LEAKED 153 MILLION ADOBE USER EMAILS, ENCRYPTED PASSWORDS, AND PASSWORD HINTS.
ADOBE ENCRYPTED THE PASSWORDS IMPROPERLY, MISUSING BLOCK-MODE 3DES. THE RESULT IS SOMETHING WONDERFUL:
USER PASSWORD
HINT
4e18acc1ab27a2d6
WEATHER VANE SWORD
4e18acc1ab27a2d6
4e18acc1ab27a2d6 a0a2876eb1ea1fca
NAME1
8babb6299e06eb6d
DUH
8babb6299e06eb6d a0a2876eb1ea1fca
8babb6299e06eb6d 85e9da81a8a78adc
57
4e18acc1ab27a2d6
FAVORITE OF 12 APOSTLES
1ab29ae86da6e5ca 7a2d6a0a2876eb1e
WITH YOUR OWN HAND YOU HAVE DONE ALL THIS
a1f9b2b6299e7a2b eadec1e6ab797397
SEXY EARLOBES
a1f9b2b6299e7a2b 617ab0277727ad85
BEST TOS EPISODE
39738b7adb0b8af7 617ab0277727ad85
SUGARLAND
1ab29ae86da6e5ca
NAME + JERSEY #
877ab7889d3862b1
ALPHA
877ab7889d3862b1
877ab7889d3862b1
877ab7889d3862b1
OBVIOUS
877ab7889d3862b1
MICHAEL JACKSON
38a7c9279cadeb44 9dca1d79d4dec6d5
38a7c9279cadeb44 9dca1d79d4dec6d5
HE DID THE MASH, HE DID THE
38a7c9279cadeb44
PURLOINED
FAV WATER-3 POKEMON
THE GREATEST CROSSWORD PUZZLE IN THE HISTORY OF THE WORLD

Title text: It was bound to happen eventually. This data theft will enable almost limitless [xkcd.com/792]-style password reuse attacks in the coming weeks. There's only one group that comes out of this looking smart: Everyone who pirated Photoshop.

## Explanation [edit]

Web sites and other computers that authenticate users via passwords need to be able to know if the user typed in the right password. But storing the password itself on the computer has been known to be unnecessarily risky since the publication of Password Security: A Case History in 1978. In that paper, Robert Morris and Ken Thompson demonstrated the practice of using a slow, cryptographically-secure one-way hash function, so that even if the password file is stolen, it will be very hard to figure out what the passwords are, so long as the passwords themselves are suitably complex. They also pioneered the use of a "salt" which makes each password hash completely different even if two users use the same password. See A tour of password questions and answers for background on salts and suitably slow hash functions.

Adobe, however, ignored these well-known principles, and instead stored over a hundred million passwords in a reversibly encrypted way, using a terrible choice of encryption methods which exposes a great deal of information about the passwords, and does not involve a salt. This password database was recently obtained by someone and released on the Internet.

In particular, Adobe used Triple DES, an older encryption algorithm which can still be relatively secure when properly used but they used it improperly. It works on 64-bit (8 character) blocks. Assuming that the passwords are stored in plain ASCII, this means that a sequence of 8 characters in a password which starts on a character position which is a multiple of eight is always encrypted to the same result. Therefore two passwords starting with "12345678" would start with the same block after being encrypted. Furthermore, this means that you can actually get a very good idea of the length of the password since anything with only one block is a password with length between 1 and 8 characters, and having two blocks implies it has between 9 and 16 characters, etc.

Adobe also stored hints users created for their passwords. That means that an attacker knows not only if the same 8 characters are used for multiple passwords but also has some hints for guessing them. That means that common password portions should be easy to recover and that any user may be "compromised" by someone else using a part of the same password and providing a good hint. As an example, a password having three hints "Big Apple", "Twin Towers" and "If you can make it there" is probably "New York" or a simple variation on that. The weakness here is that no decryption and therefore no hard cracking has to take place, you just group the passwords by their encrypted blocks and try to solve them like a crossword puzzle. These weaknesses have already been used to presumably identify a password used by Edward Snowden, as discussed at 7 Habits of Highly Effective Hackers: Can someone be targeted using the Adobe breach?.

The examples are not taken from the actual leaked file, since that uses a different format, and the examples are evidently cleverly crafted to make a nice crossword-like puzzle, which can be solved as shown in the Passwords section below.

As mentioned on http://filosottile.github.io/analyzing-the-adobe-leaked-passwords/ the data in the comic isn't real and contains a hidden message. If the "user password" hashes are Base64 encoded, they read:

```
ThiswasnotagooduseofyourtimeButthenagainitwasprobablynotagooduseofmytimeeith
erAndyetherewereareXOXOXOLetsLiveHereInThisTinySecretEncodedTextWorldForever==
```

E.g., with the initial unique hash blocks: `python -c "print '4e18acc1ab27a2d6a0a2876eb1ea1fca'.decode('hex_codec').encode('base64')"`

The last letter "r" is not fully encoded in the data shown, but any letter from "g" to "v" produces the same binary data.

The title text makes a reference to a previous comic: Black Hat's trouble with what to do with stolen passwords. It also states that users of pirated Photoshop are the winners here. This is because in order to make Photoshop pirate-able, it was modified (cracked) by removing the requirement for registration so their passwords were not sent to Adobe and therefore are not present in the leaked file.

The title itself is a reference to cryptic crosswords.

## Passwords [edit]

Note that characters in the passwords could be upper or lower case, and they may involve common substitutions like "0" (number zero) for "O" (letter O); therefore, the clues cannot guarantee that the answer shown here is precisely correct. Nevertheless, we have plenty of information for a brute force attack.

| Input | Hint | Password | Explanation |
|---|---|---|---|
| `4e18acc1ab27a2d6` | weather vane sword | `matthias` | In Redwall, several characters are associated with a sword hung from a weather vane, but only Matthias shares the name of an apostle (6 lines down). |
| `4e18acc1ab27a2d6` | | `matthias` | Although no hint was used, we know this password too, since it matches the previous one. |
| `4e18acc1ab27a2d6 a0a2876eb1ea1fca` | name1 | `matthias1` | Even without knowing the user's name, we already know how this starts, so the clue gives us a pretty good idea how it finishes (and another block useful 2 lines down) |
| `8babb6299e06eb6d` | duh | `password` | Unfortunately, this is all too common, and the user practically told us that it's an easy one. |
| `8babb6299e06eb6d a0a2876eb1ea1fca` | | `password1` | Although no hint was used, we know this by combining the previous two. |
| `8babb6299e06eb6d 85e9da81a8a78adc` | 57 | `password57` | Since we know how this begins, this is a good guess. |
| `4e18acc1ab27a2d6` | favorite of 12 apostles | `matthias` | The hint suggests only 12 possibilities. Variant spellings, variant lists, and a replacement for Judas add to that number. But we already know which one by combining with the clue 6 lines up. (Surprise: it's the replacement!) |
| `1ab29ae86da6e5ca 7a2d6a0a2876eb1e` | with your own hand you have done all this | `Judith1510` | This is a quotation from Judith 15:10 in the Bible. |
| `a1f9b2b6299e7a2b eadec1e6ab797397` | sexy earlobes | `Charlie Sheen` | This refers to an episode of *Two and a Half Men*. Other answers are possible, but only this one fits the next line. |
| `a1f9b2b6299e7a2b 617ab0277727ad85` | best TOS episode | `Charlie X` | "TOS" refers to the original series of *Star Trek*. Although this had dozens of episodes, only one fits the previous line as well as the next line. |
| `39738b7adb0b8af7 617ab0277727ad85` | Sugarland | `HoustonTX` | Sugar Land is a suburb of Houston, Texas. This fits with the previous line. Sugarland is a band, but it does not fit well with the previous hint, and would not lead to our first guess. |
| `1ab29ae86da6e5ca` | name + jersey# | `Judith15` | Even if we knew this user's name, we wouldn't know their jersey number. But the clue 4 lines up already gave us the answer. |
| `877ab7889d3862b1` | alpha | `abc` | This password is also far too common, but this clue still isn't enough to narrow it down. Combine with the clue 4 lines below, however, and it's quite easy. |
| `877ab7889d3862b1` | | `abc` | No hint, but the same as the surrounding passwords. |
| `877ab7889d3862b1` | | `abc` | No hint, but the same as the surrounding passwords. |
| `877ab7889d3862b1` | obvious | `abc` | Same as the surrounding passwords. |
| `877ab7889d3862b1` | Michael Jackson | `abc` | Michael Jackson did many songs, but only one was alphabetical (4 lines up). |
| `38a7c9279cadeb44 9dca1d79d4dec6d5` | | `asdfghjkl` | No hint, but the same as the one below. |
| `38a7c9279cadeb44 9dca1d79d4dec6d5` | he did the mash, he did the | `asdfghjkl` | Probably a "keyboard mash" (e.g. asdfghjkl), a common password. The hint is a reference to the song "Monster Mash" ("He did the mash/He did the monster mash"). |
| `38a7c9279cadeb44` | purloined | `asdfghjk` | A reference to the Edgar Allan Poe story "The Purloined Letter", this represents all the keys of the home row, or the keyboard mash password, but with one missing("purloined") letter. |
| `a8ae5745a2b7af7a 9dca1d79d4dec6d5` | fav water-3 Pokemon | `Tentacool` | This is the only water-3 Pokémon with a 9 letter name ending in "l", so it must be this to fit with the password 'asdfghjkl' |

## Transcript [edit]

Hackers recently leaked ***153 million*** Adobe user emails, encrypted passwords, and password hints.
Adobe encrypted the passwords improperly, misusing block-mode 3DES. The result is something wonderful:

```
User password                      Hint
-------------                      ----

4e18acc1ab27a2d6                   weather vane sword
4e18acc1ab27a2d6
4e18acc1ab27a2d6 a0a2876eb1ea1fca  name1
8babb6299e06eb6d                   duh
8babb6299e06eb6d a0a2876eb1ea1fca
8babb6299e06eb6d 85e9da81a8a78adc  57
4e18acc1ab27a2d6                   favorite of 12 apostles
1ab29ae86da6e5ca 7a2d6a0a2876eb1e  with your own hand you
                                   have done all this
a1f9b2b6299e7a2b eadec1e6ab797397  sexy earlobes
a1f9b2b6299e7a2b 617ab0277727ad85  best tos episode
39738b7adb0b8af7 617ab0277727ad85  sugarland
1ab29ae86da6e5ca                   name + jersey#
877ab7889d3862b1                   alpha
877ab7889d3862b1
877ab7889d3862b1
877ab7889d3862b1                   obvious
877ab7889d3862b1                   Michael Jackson
38a7c9279cadeb44 9dca1d79d4dec6d5
38a7c9279cadeb44 9dca1d79d4dec6d5  he did the mash, he did the
38a7c9279cadeb44                   purloined
a8ae5745a2b7af7a 9dca1d79d4dec6d5  fav water-3 pokemon
```

The greatest crossword puzzle in the history of the world

## Discussion

add a comment! · refresh comments!

The answer to the weathervane sword/ favorite apostle hint has got to be Matthias. It is 8 characters long, Matthias was the apostle chosen to replace Judas and in the Redwall series Matthias is one of the wielders of the Sword of Martin a sword that was hung on a weathervane.

It is unclear to me if these are actual hashes from Adobe file? That would be very cool... but actual file seems to have passwords in slightly different format. http://arstechnica.com/security/2013/11/how-an-epic-blunder-by-adobe-could-strengthen-hand-of-password-crackers/ 108.162.229.211 09:05, 4 November 2013 (UTC) pavel

I wouldn't call 3DES secure ... but yes, in this situation the real problem is not using per-user salt. Note that I would expect that at least some of those examples would be solvable ...any idea? Hmmm ... sword of weather vane and one of apostles might be Martin ([1]) ... -- Hkmaly (talk) 10:00, 4 November 2013 (UTC)

It's Jonathon (for John). Not sure what it has to do with weather vane swords though... 108.162.240.18 12:42, 4 November 2013 (UTC)

Umm. "Peter" does not seem to have 8 characters, does it? Encryption method suggests it should be 8 characters, as do 8 character boxes on the right... 108.162.229.211 10:43, 4 November 2013 (UTC) pavel

I'd say "weather vane sword", "name1" and "favorite of 12 apostles" is (Saint) Peter. "Weather vane" as symbol for the rooster in the denial, and the sword Peter used when Jesus was arrested. --108.162.254.177 10:25, 4 November 2013 (UTC)

... interesting that google search didn't mentioned it :-) Seems bible have too low pagerank. -- Hkmaly (talk) 10:32, 4 November 2013 (UTC)

The 'favourite' apostle was John the Evangelist though. http://en.wikipedia.org/wiki/Disciple_whom_Jesus_loved . The other biblical clue here is 'with your own hand you have done all this' - Judith 15:10. If that's Judith1510 then the 'name and shirt number' is 'Judith15'. The TOS/earlobes clue seems to be "Spock's brain" and "Spock's (ears?)". And the Michael Jackson one is (obviously) ABC123. 141.101.99.214 11:14, 4 November 2013 (UTC)

Perhaps "favorite" in this case refer to the user's favorite, not Jesus's. Yomikoma (talk) 16:13, 4 November 2013 (UTC)

The Michael Jackson password should just be "ABC". (The other clue refers only to letters, and the proper song title also has only letters.) —TobyBartels (talk) 20:57, 4 November 2013 (UTC)

Given that name1 is two blocks long, I would guess that the apostle's name is going to be eight characters long, with the second hash block being 1+seven spaces (or nulls if Adobe pads it with nulls and not spaces). But then again, as the only disciple with a name eight letters long is Thaddeus maybe not 141.101.99.214 (talk) (please sign your comments with ~~~~)

"St.Peter" is 8 characters, and having a "special" character (the period) makes it a good choice for passwords that might require 1 non-alphanumeric character (and ban spaces). 141.101.99.223 11:47, 4 November 2013 (UTC)

I think it is obvious that Name1 refers to (The user's name) + 1. I wonder though if we should be referring to one of the other 12 apostles in a different context? https://en.wikipedia.org/wiki/Twelve_Apostles_%28disambiguation%29 - 108.162.242.11 18:02, 4 November 2013 (UTC)

Is the "weathervane sword" referring to Redwall? I haven't read the book myself, but would it be referring to the "Sword of Martin"? [2] --Jeff (talk) 19:17, 4 November 2013 (UTC)

Another article about using passwords hints from multiple users to find the passwords from the breach. http://7habitsofhighlyeffectivehackers.blogspot.com/2013/11/can-someone-be-targeted-using-adobe.html Bugefun (talk) 11:06, 4 November 2013 (UTC)

"Sexy earlobes" makes me think of "The ABC of Aerobics", but that would make Shirley Clarke, and nothing in Star Trek has anything to do with Shirley that I am aware of, except possible Shirley Bonne as Ruth. I skimmed a list of episode titles, but nothing jumps out at me as particularly earlobish. 108.162.219.187 11:20, 4 November 2013 (UTC)

Sexy earlobes might have something to do with Ferengi, but they didn't appeared in TOS. 141.101.99.214's idea is better. -- Hkmaly (talk) 11:42, 4 November 2013 (UTC)

OK, we know that "sexy earlobes" and "best TOS Episode" are the same for the first eight character, but differ after that, while "best TOS" and "sugarland" are the same after the first 8 characters. So, my guesses are : Best TOS episode: "Charlie X"; "Sexy Earlobes": Someone with the first name of "Charlie"; "Sugarland": some city in Texas (perhaps "HoustonTX") JamesCurran (talk) 16:51, 4 November 2013 (UTC)

Note that you should not ever use cipher in ECB (electronic codebook) mode, i.e. encrypt each block separately and independently, but use chaining. --JakubNarebski (talk) 12:15, 4 November 2013 (UTC)

And for passwords you shouldn't be using a cipher at all, but rather a hash function. (Or a cipher in one of the approved hash constructions, if you must.) And really you shouldn't be using a standard hash function, but be following best practices for passwords instead: salting the hash, using a *slow* hash function, etc. Cscott (talk) 20:22, 4 November 2013 (UTC)

Hmm, i'm rather confused about the last few on the list though. Assumedly the password for "he did the mash, he did the" would be "monster mash", but that would leave "purloined" with a password of either "monsterm" or "monster ". which doesn't make much sense. 108.162.240.18 13:47, 4 November 2013 (UTC)

(charlie sheen) a1f9b2b6299e7a2b eadec1e6ab797397 sexy earlobes - He did a 2 and a half men episode on sexy earlobes

(charlie x) a1f9b2b6299e7a2b 617ab0277727ad85 best tos episode - Star Trek has so many good episodes...

(houstontx) 39738b7adb0b8af7 617ab0277727ad85 sugarland - Sugarland is in Houston, TX

I don't know about anyone else, but the "hints" column incidentally reminded me of Darwinian Poetry. Not intentionally, I'm sure. 141.101.98.214 14:46, 4 November 2013 (UTC)

Somehow I've missed out on this issue until this comic alerted me to it, but: once a few passwords are correctly guessed, does that make it straightforward to recover the encryption key, and then be able to decrypt **all** of them? —scs (talk) 14:50, 4 November 2013 (UTC)

Answering my own question: not really straightforward, no. 3DES is still pretty strong, and what knowing a few passwords gives you is a known-plaintext attack, which helps a little, but is by no means a giveaway. —scs (talk) 15:00, 4 November 2013 (UTC)

Note that if blackhat used this service, he would know at least one plaintext - his own password--JakubNarebski (talk) 15:05, 4 November 2013 (UTC)

No, for calculating the encryption key of Triple DES, there is no real benefit in knowing million passwords, you would still need to brute force it. You would need to know at least $2^{32}$ different passwords to make it easier but you can't do that with the leaked file (there are about 30 times less of them and moreover many of them are not unique). Sten (talk) 16:08, 4 November 2013 (UTC)

Okay, so the first column is the encrypted password, the second one is the hint chosen by user. What do rectangles mean? 173.245.53.151 15:28, 4 November 2013 (UTC)

That are the fields to fill the characters in just as you do in a crossword puzzle. There are small fields at the beginning that take one character each and one large field at the end that takes one to eight characters. Sten (talk) 15:32, 4 November 2013 (UTC)

Water 3 is an egg group: http://bulbapedia.bulbagarden.net/wiki/Water_3_(Egg_Group) . Given the length of the key, it will probably be 9-16 characters. (Crawdaunt, tentacool, and tentacruel are most likely) 199.27.128.139 15:43, 4 November 2013 (UTC)

-- which means 9dca1d79d4dec6d5 is either L, EL, or T, but I can't find a way for that to match up with any variation of "monster mash." 173.245.55.209 16:15, 4 November 2013 (UTC)

Same problem here... Monster mash must not be correct, but it is one of the easier ones, I can't give up on it. --Jeff (talk) 17:35, 4 November 2013 (UTC)

Maybe, he did the MASH is about the book, movie or TV Show M*A*S*H instead? --Jeff (talk) 17:49, 4 November 2013 (UTC)

Monster Mash was written by Bobby Pickett, maybe it has something to do with him? Sten (talk) 18:38, 4 November 2013 (UTC)

Maybe it's not "monster mash" but just "monster". This would allow the Water-3 Pokemon to be "Cloyster". 108.162.237.5 19:17, 4 November 2013 (UTC)

You are having trouble counting to eight. Cscott (talk) 20:22, 4 November 2013 (UTC)

You are forgetting the space. Assuming space is stored as a null character, this might actually work.173.245.54.29 01:43, 5 November 2013 (UTC)

Nobody in their right mind would encode spaces as nulls. For us to suppose that they did, we'd need to have some specific clue to that effect. 108.162.238.5 09:08, 5 November 2013 (UTC)

It seems to me there are two puzzles here, if folks are right that this is not actual data from the hack. 1) Figure out Adobe's master 3DES encryption password, for the big prize. 2) figure out Randall's 3DES encryption password for this puzzle based on these hints, and knowing it will be something clever. Nealmcb (talk) 16:12, 4 November 2013 (UTC)

Trying to decode the passwords (As Randall obviously wants us to) "with your own hand you have done all this" is from the book of Judith. Working on decoding the others. --Jeff (talk) 17:13, 4 November 2013 (UTC)

8babb6299e06eb6d = password a0a2876eb1ea1fea = 1 85e9da81a8a78adc = 57 --Jeff (talk) 18:10, 4 November 2013 (UTC)

Weather Vane Sword may be a reference to Game of Thrones Ascent. The "Sworn Sword", I believe is "Rona" which is also a name. 173.245.55.216 18:27, 4 November 2013 (UTC)

It needs to be a name of an apostle (as per line 7) and have 7 or 8 characters (as line 3 needs a continuation) so this leaves Matthew, Thaddeus and (Judas) Iscariot. Sten (talk) 18:57, 4 November 2013 (UTC)

If a password(or 8 character segment) is guessed can it be confirmed? Somebody should take this leaked list and create a website that presents it like in the comment and lets people guess. It can fill in the guessed ones. 108.162.246.117 19:17, 4 November 2013 (UTC)

I'm putting in Mattias for the sword, name1 and disciple because of Saint Matthias [3] and Redwall Matthias [4] who held the Weathervane Sword (Also known as the sword of Martin [5] ) --Jeff (talk) 19:27, 4 November 2013 (UTC)

I've also removed "monster mash" from the list as it can't be right. Doesn't match the pokemon or the purloined clues. --Jeff (talk) 19:27, 4 November 2013 (UTC)

Based on the Water-3 Pokemon hint, the only possibilities of more than 8 characters are tentacool, tentacruel, barbaracle, crawdaunt, carracosta, clauncher, and clawitzer. This would mean "9dca1d79d4dec6d5" would be l, el, le, t, ta, or r. --Dvorakmd (talk) 19:51, 4 November 2013 (UTC)

This is assuming there are no characters before the actual name of the pokemon. 173.245.55.209 20:30, 4 November 2013 (UTC)

Assuming Randall has constructed this comic to have a unique answer, it can't end in r because then the clue would be ambiguous (could be clauncher or clawitzer). Cscott (talk) 21:53, 4 November 2013 (UTC)

Some of these can be ruled out; it's very unlikely to be a Generation VI Pokémon (Barbaracle, Clauncher and Clawitzer) as this has only just come out and someone would have had to set up their password within the last few weeks. And the Pokémon that are also in the Water-1 group are probably more likely to be thought of as Water-1 than Water-3 (Crawdaunt and Carracosta). This only leaves Tentacool and Tentacruel as longer than 8 letter Water-3 only Pokémon that have been known of for a reasonable length of time; and Tentacool is no one's favourite, as the annoying multitude of them that show up whenever you try to Surf anyway makes them as reviled as Zubats in caves, if not moreso. :P Of course, the password need not be simply the Pokémon's name alone. "SexyShellder" "Cloyster1987" "Misty'sStarmie"... Who knows? 141.101.99.252 01:03, 5 November 2013 (UTC)

I don't know the answer to the end either, but here's a list of people who did the Monster Mash, from Wikipedia:

- Bobby Picket (as Boris Picket)
- Garpax Records (Gary S. Paxton)
- The Misfits
- far, far too many other covers to list

And here's some synonyms for "purloined", from thesaurus.com:

- stole
- pilfered
- filched
- misappropriated
- embezzled
- burglarized
- shoplifted
- poached
- pillaged
- cheated
- pinched
- heisted
- thieved
- plundered
- appropriated
- lifted
- took
- snitched
- defrauded
- swindled
- ripped off
- made off with

Good luck with these! —TobyBartels (talk) 20:31, 4 November 2013 (UTC)

What about Purloined referring to "The Purloined Letter?" When choosing hints, people, at least in my experience, tend to use word association rather than synonyms. 173.245.55.209

Purloined could also be a reference to the Monster.com hack (http://www.symantec.com/connect/blogs/monster-trojan). 108.162.237.11 21:00, 4 November 2013 (UTC)

Words meaning purloined that can have the listed suffixes could be **embezzle/embezzler** or **scrounge/scrounger**. Not sure if it fits to the mash clue. There was a loan shark character who would acquire things on MASH called Rizzo, it is a stretch though. 108.162.246.117 21:01, 4 November 2013 (UTC)

I'm still trying to figure out how the solutions go into the spaces on the right -- it may be more obvious once the last couple clues are figured out. I suspect the ordering and numbers of clues have some sort of meaning. Why are there 5 of the 877... passwords, 2 with no clues? Why is one of the 4e18.... passwords separated from the rest? 108.162.221.28 21:07, 4 November 2013 (UTC)

Could Purloined be a reference to the "Purloined Shadows" book in Elder Scrolls? --Dvorakmd (talk) 21:09, 4 November 2013 (UTC)

Or 'The Purloined Payroll', a WoW quest? "Purloined in Petrograd" is also a lyric to a Decemberists song (The Bagman's Gambit). Google n-grams suggests that "Purloined Image", and "purloined documents" are a Thing. Cscott (talk) 21:58, 4 November 2013 (UTC)

Purloined could be a reference to something that is known as have been stolen like a work of art, or it could be something that was stolen in an XKCD comic. 108.162.246.117 21:18, 4 November 2013 (UTC)

**EdgarPoe**(author of The Purloined Letter)/**EdgarPoet** fits, but again not really anything to do with MASH. 108.162.246.117 21:27, 4 November 2013 (UTC)

Water-3 pokemon (egg group) are given here: http://bulbapedia.bulbagarden.net/wiki/Water_3_(Egg_Group) ...if I split off the letters of their names after the 8th letter, we see l, el, le, t, ta, and r. So the MASH item ends with one of those suffixes. 199.27.128.167 21:31, 4 November 2013 (UTC)

Can't end in 'r', because then that clue would be ambiguous. Cscott (talk) 21:53, 4 November 2013 (UTC)

Speaking of pokemon, could the clue to purloined have something to do with the pokemon Purrloin? http://bulbapedia.bulbagarden.net/wiki/Purrloin_(Pok%C3%A9mon) 108.162.221.43 23:51, 4 November 2013 (UTC)

Is there a reason "MASH" is capitalized in the above sections? Given the context, it shouldn't be, and I still haven't given up on the password being a reference to the monster mash. That said, we can't ignore the movie/show MASH. Also, now that I think about it: pokeMONSTermash? I don't know, just throwing ideas out :P 173.245.55.209 22:08, 4 November 2013 (UTC)

On reddit they suggest "Letterman" (which is wrong, too many letters) based on the M*A*S*H episode, "Letters". Cscott (talk) 22:11, 4 November 2013 (UTC)

...on the other hand, I wonder if an answer like "ALANALDA" would work? As in, someone who "did the M*A*S*H"... Cscott (talk) 22:13, 4 November 2013 (UTC)

Sadly, no. Because it needs to be more than 8 characters. --Jeff (talk) 22:17, 4 November 2013 (UTC)

No, I mean, "an answer of this form", not ALANALDA exactly. The Edgar Allan / Alan Alda congruence is tasty, but I can't make it work. ALLANPOE works as an answer for "Purloined" but that makes something like ALLANPOET the answer to "he did the MASH" (CRAWDAUNT is then the pokemon). But that's misspelling Alda's name for the MASH clue, doesn't quite work. There's also JAMIEFARR (Cpl Klinger) as a better answer to "he did the MASH" but then that makes JAMIEFAR the answer to "purloined" and I can't plausibly make that work. ALLANARBUS is another M*A*S*H actor, but that doesn't work at all. Can anyone come up with other/better ideas in this vein? Cscott (talk) 22:31, 4 November 2013 (UTC)

Don't misspell Alda's name; misspell Poe's! —TobyBartels (talk) 02:07, 5 November 2013 (UTC)

In crossword puzzles, a clue ending in -ed (like 'purloined') is most commonly a hint that the answer ends in 'ed'. Cross referencing that with the Pokemon clue, the solution for "he did the MASH" becomes a nine or ten letter answer ending in: -edl, -edel, -edle, -edt, or -edta (excluding -ed due to non-uniqueness), with ......edle looking the most "English-y" to me. My hunch would be something else Robert Altman or Alan Alda "did"... but nothing seems to end in 'edle.' --Willowy burrito (talk) 23:07, 4 November 2013 (UTC)

There is no indication that this is a standard crossword. Most users don't respect crossword conventions when writing password hints. Cscott (talk) 23:59, 4 November 2013 (UTC)

Aside from the title. And the text. And the fact these didn't come from users, but were just chosen for a puzzle designed by Randall, who would include just this sort of puzzler hint/in-joke in a comic about puzzles. It's moot, because no synonyms for 'stolen' make any sense with a couple other letters tacked on the end. But still, there've been worse hunches. --Willowy burrito (talk) 00:45, 5 November 2013 (UTC)

For all we know, his favourite Water-3 Pokémon could be Shell Smash Cloyster or Shell Smash Omastar - "OmastarSmash" as a password would fit in with "Monster mash". 141.101.99.252 23:16, 4 November 2013 (UTC)

I like that idea, although it leaves "Monster " (with a trailing space) as the answer to "Purloined", which makes no sense. But interesting idea. Cscott (talk) 00:00, 5 November 2013 (UTC)

MonsterMash MonsterM TheWiscash Jcupcake (talk) (please sign your comments with ~~~~)

It's "Whiscash", and it's Water 2 (not 3) and "MonsterM" makes no sense as an answer for the hint "Purloined". But I like the idea of adding "The" in front of the pokemon answer; perhaps we're being too restrictive by looking only at pokemon with length > 8. Cscott (talk) 23:59, 4 November 2013 (UTC)

Yeah, sorry about the typo - last one would be TheWhiscash. MonsterM absolutely makes sense. http://www.hoax-slayer.com/monster-666.shtml The purloined letter here IS M Jcupcake (talk) 02:40, 5 November 2013 (UTC)

So somewhere above this someone pointed out that purloined could refer to a monster.com hack...in which case, could the first two passwords be "monster mash" and "monster"? That would allow for another previous suggestion of "OmastarSmash". Also, here's my IP Address and a remarkably not-random timestamp: 108.162.219.195 01:31, 5 November 2013 (UTC)

It could also be that there are modifiers to the base. I always thought of Monster Mash as MonstaMash. This would line up closely with My Corphish written as "mycorphish" My favorite pokemon is my pikachu not just any pikachu, but mine, sort of logic. Bitassassin (talk) 01:43, 5 November 2013 (UTC)

Could "he did the mash" be referring to brewing and/or the Maillard reaction? Cscott (talk) 05:32, 5 November 2013 (UTC)

I was just thinking that "MonsterM Ash", "MonsterM", both seem to make sense, and Ash had a few water pokemon in the water 3 egg group, so could it potentially be something along the lines of "Corphish Ash"? That was the only 8 letter water 3 pokemon he had and it fits with the other clues NewToThis (talk) 07:25, 5 November 2013 (UTC)

Has the idea of pokemon fusion been considered? http://pokemon.alexonsager.net/ referenced by http://kotaku.com/how-the-website-that-lets-you-create-frankenstein-pokem-510517336 -- Oukansz (talk) 19:25, 5 November 2013 (UTC)

**Fanservice**

Randall must know about this site. This comic doesn't work without people to crack the code. Should we have a fanservice category? :-) --SurturZ (talk) 23:32, 4 November 2013 (UTC)

I'm beginning to suspect that the wide boxes will have the key in it. Assuming he used regular DES (or DES3, for that matter, but using the same 8-byte key 3 times), it could be plausible. The 5 in the middle could be 'abcde', a lot of the other 'second halves' are numbers, and the likely known one that's not seems to be an 'x' -- which could certainly be involved in writing a hex number... problem is there's 11 of those boxes. Trying to guess what signficance the positioning of those boxes have. 108.162.221.28 00:00, 5 November 2013 (UTC)

Actually, it looks like the boxes line up perfectly such that the wide bits (for second-half) will only touch the words they apply to. Order will be more or less what they are (I see the wide boxes as, in order, 1, 57, 10, Sheen, and X, with the 8 char boxes as Matthias, Password, Judith15, Charlie, and HoustonT). The next 5 are odd -- I'm not sure if we repeat the alpha/obvious password 5 times, or it's 5 chars long (abcde) and one per box. The last set is still under discussion, of course. 108.162.221.28 00:20, 5 November 2013 (UTC)

**MASH capitalized**

I'm currently chasing down the idea that MASH refers to Wikipedia:MASH-1. Haven't seen any name yet that looks like it might satisfy "Purloined". - BozoTheScary (talk) 01:56, 5 November 2013 (UTC)

I think MASH is a transcribing error. The comic doesn't have any difference on those letters as far as I can tell. 173.245.50.222 03:18, 5 November 2013 (UTC)

The Purloined Letter is a Edgar Alan Poe story starring C. Auguste Dupin. Might help. 108.162.249.5 03:08, 5 November 2013 (UTC)

There is also a strong association between the Monster Mash and the Mashed Potato, just throwing another idea into the ring. Also try the name BobbyPickett. 108.162.249.5 03:22, 5 November 2013 (UTC)

Frankenstein did the Monster Mash in the cartoon for the song. That leads to a Pokemon card ending in 'tein' and 'frankens' for the hint Purloined. I could not find a Pokemon card that ended in 'tein' nor could I link 'frankens' with Purloined. I ran 'frankens' through Google Translate but found nothing. Also, it's the same password for the "monster mash" hint and the entry with no password hint so I think it's an obvious password (something someone can recall without a hint). Frankenstein fits that part but not the other ones. 173.245.50.222 03:35, 5 November 2013 (UTC)

My $0.02: "He did the mash..." might allude to the expression "doing the math" only (intentionally) misspelled and something like "numbert" or "numb" could be the answer. --RagnarDa (talk) 04:01, 5 November 2013 (UTC)

graveyard smash fits for the first clue (though lyrically incorrect). Gives smash as second block, but cannot find association between graveyard and purloined. 108.162.249.5 04:08, 5 November 2013 (UTC)

If we take The Monster Mash for the first answer, it could be written as TheMonsterMash or The Monster Mash, giving either TheMonst erMash or The Mons ter Mash as the two blocks. This gives either Themonst or The Mons as Purloined and either ermash or ter Mash for second block of pokemon answer. Suggestions? 108.162.249.5 04:15, 5 November 2013 (UTC)

Only problem is that the word "the" is the last word of the hint.108.162.237.117 04:51, 5 November 2013 (UTC)

I know that the water-3 group is not the same, but it seems like an odd coincidence that another pokemon group is the "monster" group. --Natnee (talk) 04:44, 5 November 2013 (UTC)

There is a Scooby Doo comic book story titled "[The Purloined Poe-M](http://scoobydoo.wikia.com/wiki/The_Purloined_Poe-M)", which has an odd similarity to the "MonsterM" possible password. This would leave the pokemon password ending "ash" who, of course, is a pokemon character ... which makes no sense in that place. 199.27.128.83 05:51, 5 November 2013 (UTC)

Here's one that fits:
facemash4077 (Combination of facemash by zuckerberg and M*A*S*H)
facemash (Site made by Zuck in The Social network.)

Maybe facmashklinger.. The eggklinger being a water-3 Pokemon? 108.162.215.39 06:14, 5 November 2013 (UTC)rbnm

John Orchard played in M*A*S*H and also was in the movie "The Letter" 108.162.250.8 05:02, 6 November 2013 (UTC)

**Working Backwards**

I'm attempting to take a different tact, by trying to find the key itself. I'm assuming its something easy to guess. I've tried the top 100 Adobe passwords (you can get them here) using the following bash script (testing the word "matthias", as this one seems pretty certain):

```
while read p; do echo -n $p\: && echo -n "matthias" | openssl enc -e -des-ede3 -nosalt -nopad -pass pass:$p | xxd -p; done < passwords.txt
```

For this to work, I pre-processed the top 100 passwords file with:

```
cat adobe-top100.txt | cut -c51- > passwords.txt
```

...and then trimmed the cruft with a text editor (leading text paragraph and table headers). So far no luck; perhaps someone with more time on their hands can try some obvious XKCD-related passwords (I've tried XKCD, xkcd, xkcd.com, randall, rmunroe, encryptic, and Encrytic) and see if the encrypted version(s) match up with what we have here. Yaztromo (talk) 09:27, 5 November 2013 (UTC)

I should mention that I've also tried OpenSSL's des-ede mode and des-ecb, as Im not sure if Randall used one, two, or three key mode. I'm also assuming the key has been generated from the password using OpenSSL's default key generation method, any of with I suppose could be incorrect. Yaztromo (talk) 09:39, 5 November 2013 (UTC)

Nice work. Note that the puzzle is very specific about using "block mode 3-DES" (usually called "ECB"). DES keys are actually 56 bits; each of the 8 bytes has odd parity (the number of 1 bits is odd). From wp, "Bits 8, 16,..., 64 are for use in ensuring that each byte is of odd parity." As a wild guess, I'd suggest that, if Randall chose a readable 8-ASCII-character passphrase, he also selected only characters that would make the parity bit zero (so that the result was ASCII). That is, `[ #%&)*,/12478;=>@CEFIJLOQRTWX[]^abdghkmnpsuvyz|]`. Cscott (talk) 16:34, 5 November 2013 (UTC)

Uh, hold one. Read the "Explanation" section above. It's clear that the hashes are not real, so brute-forcing the key isn't going to work. Cscott (talk) 16:48, 5 November 2013 (UTC)

Just to note, there are actually three options for keys in TripleDES: having three independent keys (K1, K2, K3), having two independent keys (K1, K2, K1), or using a single key (K1, K1, K1). When run in ECB mode, OpenSSL calls these **des-ede3** and **des-ede** for options 1 and 2 (option 3 is for backwards compatibility with DES, and can be run using just **des-ecb**). See Triple DES - Keying Options for details. In addition, the password and the key are two different entities -- typically the password is run through a keying algorithm first (commonly PBKDF2 for 3DES), so there is no need to select password characters based on parity patterns. All of which is moot now that we know that the data isn't in fact TripleDES encrypted in the first place. I'm actually disappointed in Randall now :P. Yaztromo (talk) 19:01, 5 November 2013 (UTC)

I Hadn't seen it mentioned yet, but Monster Mash was written by Robert George Pickett (http://en.wikipedia.org/wiki/Bobby_Pickett), Whose last name goes closely with the second clue, Purloined, which means "stolen". I can't make it work, but I figured it was worth pointing out. (Nov 5th 1:26 pm utc ) 173.245.56.24 13:27, 5 November 2013 (UTC)

It's a good connection. Maybe we should reorganize the discussion and start a list of "interesting ideas we can't quite make work" in the hopes that someone else has an insight. Edgar Allan / Alan Alda, Pickett / "Pick it", Klinger / Kingler, etc. Most of these are just manifestation of the human brain's ability to find patterns even in random coincidence, of course, but one of them might be on the right track. Cscott (talk) 16:23, 5 November 2013 (UTC)

Just quick thoughts. I feel like Cpl klinger and the water type kingler is too solid a connection to ignore even though I can't really use it. Kingler was owned in the series by Ash. Ash is a three letter word and the last three letters of the phrase monstermash. Monsterm=8 letters so the first block ash=3 letters in the second block. Monsterm is about the monster.com thing, therefore purloined. It's a double reference, the .co has been purloined from the purloined website. Then blastoise -3, or rather blastois3 - 3 (mocking the common password meme of replacing letters with numbers) So the last password, which is super hard to guess and well chosen even with the clue is, blastoisash? It's a feasibly memorable password that would not be quickly forgotten by a pokemon fan while still being hard to guess. Can you think of a way to check it? Maybe go into the old command line xkcd and try it as a password? (From a contributor to my talk page) --Jeff (talk) 13:52, 5 November 2013 (UTC)

That's really a stretch. ".co is purloined from monster.com?" really? The answer will be far more obviously correct... once we figure it out. Look at the other answers, for example. Cscott (talk) 16:23, 5 November 2013 (UTC)

**another quick idea for monster mash**

It could be deflection. Maybe whoever put it in was paranoid. Or just dumb. Or who knows.

But, there is a pokemon that's in the monster/water(-1) hybrid group called Marshtomp.

Monster mash, mashed (ie anagrammed) can give us all but the P out of that... which is fine, as it's a 9-letter name.

Thus we have E, N and S left over (and indeed a further T, H, E), which could become overall, e.g, Marshtomens (...Marshtomethens? Or w/e), which you can split up as you like to represent something which has been stolen (personally). Possibly in german slang or something. It doesn't have to be a direct thesaurus link, it could well be complete misdirection (on Randall's behalf, or that of his notional Adobe user), same as for the pokemon.

And for the pokemon itself, it could well be "Marshtomp3" ;)

Also, don't forget about reversed words and so-on.

Heck, I've used very personal and/or random things (like, maybe two or three people in the world may recognise it in connection with me, and it's not online, at least not anywhere it can be found - basically it's just in my head and dies with me), reversed, with numbers substituting random characters, as passwords before. That covers each individual base in just one PW...

Now we just have to start feeding the guesses into a hash engine and try to figure out, maybe brute force, what the original key was. Knowing almost all of the other answers already makes this far, far easier for those who may have the facility to run the tests already. 141.101.99.213 14:54, 5 November 2013 (UTC)

This is not a real excerpt from the password file, this is a puzzle which Randall made up. Therefore, the answer to the last group will not be random, and it will not be a stretch. It will be obvious (as obvious as the previous ones)... once we figure out the catch. Cscott (talk) 16:23, 5 November 2013 (UTC)

FWIW, Eve Online also features a "Purloined Sansha Codebreaker". Cscott (talk) 17:16, 5 November 2013 (UTC)

I agree that the solution has to be obvious - especially after its revealed. If this were a crossword puzzle, then the clues like Purloined might be followed by a question mark. Purloined? a cat that is loined - a cat that is covered with cloths? Puss in boots? Or something along those lines... 108.162.215.34rbnm

purloined=phished (Corphish)? 108.162.216.227 (talk) (please sign your comments with ~~~~)

i wonder if the link between the last three clues is more like a cryptic crossword puzzle--for instance, --purloined= heisted; the other clues reading it as he/is/ted...?--Wwd (talk) 22:40, 5 November 2013 (UTC)

I wonder if the pokemon could be the name of an ubuntu release, per "Not Really Into Pokemon" at http://xkcd.com/178/ --Willowy burrito (talk) 22:45, 5 November 2013 (UTC)

You could also abbreviate Robert Pickett's name (the co-writer of Monster Mash) as "Rob Pickett" which goes even more with purloined (the first 8 letters are now "Rob Pick"). Davheld (talk) 06:21, 6 November 2013 (UTC)

Beings that "did the mash" according to the song http://www.lyricsondemand.com/onehitwonders/monstermashlyrics.html : my monster, the ghouls, Igor, Igor's baying hounds, the coffin-bangers, "The Crypt-Kicker Five", you. Zombies, Wolf Man, Dracula/Drac, and Boris were also mentioned, but they didn't do the mash. Hope that helps someone (doesn't help me). DPWally (talk) 23:05, 6 November 2013 (UTC)

**Capitalization hints?**

I have no idea who first put the capital letters in "MASH" and "Purloined" in the transcript (and I don't want to check), but now that I've gotten rid of the second (after somebody else got rid of the first), I want to record them here for the record. Possibly Randall put them in and was feeding us clues (so *MASH* the book or movie, and *Purloined* a title such as Poe's). I consider this unlikely (after all, I removed one of these capitalizations), but the possibility should be recorded. —TobyBartels (talk) 01:17, 6 November 2013 (UTC)

I can't be a coincidence that this comes up as the top google news search for 'purloined:' http://www.theregister.co.uk/2013/11/05/adobe_users_purloined_passwords_were_pathetic/ 108.162.246.120 (talk) (please sign your comments with ~~~~)

"38a7c9279cadeb44 9dca1d79d4dec6d5 he did the mash, he did the": Ministermash (sounds like monster mash) "38a7c9279cadeb44 purloined": Minister (based on the character Minister D-, who stole the letter in the Edgar Allen Poe story) "a8ae5754a2b7af7a 9dca1d79d4dec6d5 fav water-3 pokemon": OmastarSmash (Shell Smash Omastar) So,38a7c9279cadeb44 = minister, 9dca1d79d4dec6d5 = mash, a8ae5754a2b7af7a = omastars 04:07, 6 November 2013 (UTC)

Probably one of the best complete theories I've heard Davheld (talk) 06:26, 6 November 2013 (UTC)

I suggest "alligato" (a form of Latin *alligatus*, perfect passive participle of *alligo* "bind up"), and "alligator" (Referencing "Land of 1000 Dances"). 199.27.128.62 05:37, 6 November 2013 (UTC)

I think there is a transcribe mistake.
Instead of "fav water-3 pokemon"
Could it be "fay water-3 pokemon"
Look at the Y and V letters in the non-chopped letters above. I think it is a Y and not a V.

```
108.162.215.51 (talk)  (please sign your comments with ~~~~)
```

- About the Pokemon, is it possible everyone's ignoring a much simpler explanation? Every Pokemon game begins with a choice of one of the three starter Pokemon, each of which have an evolutionary line of three Pokemon. In first gen, if your "favorite [is] water [from the] 3 Pokemon", then you'll be using Squirtle, followed by Wartortle and Blastoise. 2nd gen: Totodile, Croconaw, Feraligatr. 3rd gen: Mudkip, Marshtomp, Swampert. 4th gen: Piplup, Prinplup, Empoleon. Perhaps the answer uses one of these, or some combination of them? --Anon 08:57, 6 November 2013 (UTC)

Boris Blacher wrote an opera based on 'The purloined letter' This may fit with Bobby 'Boris' Pickett who sang Monster Mash YellowYeti (talk) 11:11, 6 November 2013 (UTC)

The "Boris" in "Boris Pickett" is a reference to Boris Karloff. (In his other work, Pickett doesn't use that name.) —TobyBartels (talk) 12:36, 6 November 2013 (UTC)

An alternative tack: how about Barbaracle for the Pokemon, BarbaraC(Jordan) for purloined and Barbara Clark - famous for doing Monster Mash-up novels. Does Barbara Jordan have some purloined link with watergate? 108.162.231.16 (talk) (please sign your comments with ~~~~)

```
 No, because the pokemon has a different starting string as the other two.  --199.27.128.119 13:48, 6 November 2013 (UTC)
```

I think it is not coincidence that it is the last one that you can't solve. It may be an experiment by Randall to see if people can find a solution for a puzzle that doesn't make any sense. That said, if it does have a solution, it should not be "monstermash" since that is too close to the clue. If that was the password, everyone could guess it easily from the clue. It has to be one level "removed" from those words, guided by the clues for the matching passwords. The point of the post was that using unsalted crypt in the passwords allows you to combine clues, right? 108.162.219.201 13:42, 6 November 2013 (UTC)

Not an answer, but maybe an approach: Look at it from the "what piece of information is Randall trying to tell us?" angle. In the first few puzzles, he teaches us the rules of the game. We disambiguate clues by later ones, which we can only do because of the missing salts. For example, the "name and jersey number" just tells us the format of the answer to the previous clue about Judith 15:10. Otherwise, there would have been no way to guess that exact string without the space and colon. Also, "Charlie X" and "Charlie Sheen" demonstrate that spaces are used in a "fair" way. I would not expect a trailing space on a password, for example. So what about the Pokemon then? The first half of the crypt for the Pokemon isn't used anywhere else. The easiest interpretation I can come up with is that this is just trying to restrict the common second part of the word to letters from the list of Water-3 Pokemon. Let's assume it wasn't made very difficult, so take just 'el', 'le', and 'l' from the Water-3-only group on bulbapedia. Then the puzzle is this:

```
something related to 'monster mash': 8 letters plus the ending 'el', 'le', or 'l'
something related to 'purloined' or related to 'letter': the same 8 letters, minus the ending
pokemon: completely unrelated, just chosen to have a well known list of 9 or 10 letter words to restrict search space for first line
```

I suck at crosswords, but can someone solve this restated version? There can't be that many 8 letter words that also make a word with 'el', 'le', or 'l' added to them? 15:23, 6 November 2013 (UTC) 108.162.219.201 (talk) (please sign your comments with ~~~~)

Not to insult your reasoning, which is entirely correct, but I believe your restatement is *exactly* the puzzle that (reasonable) people have been working on (and failing to solve) since Monday. As a long-time mystery hunter, I'd like to suggest the opposite: the continued failure to find some reasonable solution to the puzzle as stated above implies that *at least one* of the assumptions above is wrong. (For the record, I'd broaden your first to "...related to 'monster mash' or the show/film M*A*S*H", but again, that's the assumption we *have* been making.) So I'm especially interested in ideas *different* from the above, at this point, although not necessarily throwing out the bathtub, baby and all. Probably there's a fundamentally different way to read the first clue, or the second, or the third. Cscott (talk) 17:11, 6 November 2013 (UTC)

Not insulted at all, just glad if I summarized it correctly, since I was late to the party. Maybe this helps others bootstrap. As requested, a slightly alternate view for clue 1: the word "mash" may not be part of the answer, since it appears in the clue. This means the direct answer to the clue is "monster" and has nothing to do with the song at all. The password could just be the name of a monster that is formed from something purloined plus an short ending. The endings we're already considering make nice monster names.108.162.219.198 19:54, 6 November 2013 (UTC)

I appreciate the summary, it helped me come up with my "keyboard mash" proposed solution, which you can see below" 108.162.221.16 21:51, 6 November 2013 (UTC)

Looking at some word lists at http://www.litscape.com/words/ending_with/l/9_letter_l_end_words.html , this doesn't seem to be leading anywhere good. Can someone fix my logic? 108.162.219.201 15:33, 6 November 2013 (UTC)

Not sure if anyone else has pointed out yet, but there is a pokemon named purrloin http://bulbapedia.bulbagarden.net/wiki/Purrloin_%28Pok%C3%A9mon%29 . That seems like far too much of a coincidence to not be related. 173.245.52.211 16:17, 6 November 2013 (UTC)

We'll add it to the long list of suspicious coincidences. Cscott (talk) 17:11, 6 November 2013 (UTC)

I don't believe the hints can be related. Note that the Pokémon's name shares zero characters with the answer to the 'purloined' clue, so they are not linked via the same password. Any semantic link is inconsistent with these being password hints from separate (imaginary) users. Maybe Randall subconsciously (or via google) went from purloined to Purrloin to names of Pokemon. 108.162.219.198 19:20, 6 November 2013 (UTC)

a stretch.. but maybe a starting point? bootlegd purloined bootlegd ash he did the.. ???whisc ash fav-3 108.162.215.34rbnm

**Hash collision**

Maybe the last clues could be intended to be a hash collision? With 64-bit blocks that seems unlikely, but maybe it's a trick? Quantum7 (talk) 21:29, 6 November 2013 (UTC)

Finding the probability of a collision amounts to the birthday problem. Assuming the hash function gives all 2^64 hash values with equal probability and there are 153 million unique message blocks (probably right within an order of magnitude), we have:

```
Pr[collision] = 1 - exp(-153000000^2/(2*2^64)) = 0.000634
```

So the probability of a hash collision from different passwords is still quite low, even with such a large number of passwords. So it's worth assuming that all the identical hash blocks are from the same message, and keep looking for the poke-mash password.
BTW, getting a 50% chance of a collision requires about `sqrt(-2^65*ln(.5))` = 5 billion unique passwords.
Quantum7 (talk) 21:46, 6 November 2013 (UTC)

**Explanation for the last 3 - Keyboard Mash**

"He did the mash, he did the" keyboard mash ASDFGHJK - L

"purloined" letter, as in one letter from the home row ASDFGHJK

Then the third one is TENTACOO - L 108.162.221.16 21:45, 6 November 2013 (UTC)

Purloined seems like a stretch. On the other hand, 'asdfghjkl' is the 56th most common password in the real adobe data, so perhaps you're on to something. Quantum7 (talk) 22:08, 6 November 2013 (UTC)

I don't know, I feel like purloined has got to be a reference to the Poe story. The pun that letter means single character rather than item of correspondence is cute and funny. 108.162.221.16 22:30, 6 November 2013 (UTC)

I like this explanation --Lackadaisical (talk) 22:28, 6 November 2013 (UTC)

This get's my vote. There's no reason for the "mash" password to be repeated twice in the puzzle with no clue for one of them except to say "this is a commonly used password" (as shown by the abc and password1 entries). Common password with an l (or el etc.) missing from the end, a purloined letter(!), plus "mash" as a clue is oblique but not crazily so 141.101.99.223 17:37, 7 November 2013 (UTC)

I agree with the repetition part. Looking at the adobe top 100 passwords http://stricture-group.com/files/adobe-top100.txt I was hoping that 'asdfghjkl' was 2/5 as common as 'abc', based on the number of repetitions. It is actually more common, but at least it is on the list. I also think it is by far the best fit if choosing only from that list. Also, maybe Randall used another source material where it is less common than 'abc.' 173.245.52.158 13:13, 8 November 2013 (UTC)

I think this is the best wrong answer yet. That is, I don't see how you can plausibly clue "ASDFGHJK" with "purloined" (that is, the hint doesn't work on its own, it requires the rest of the puzzle to make sense at all, which is against the rules of the puzzle). But it's a good story. Definitely wrong, but wrong in a really interesting way, and the most interesting wrong answer yet. ;) Cscott (talk) 19:41, 7 November 2013 (UTC)

I disagree. Even without the context of the rest of the comic, ASDFGHJKL is such a common password that it makes sense to imagine a hint that simply refers to a variation on it. In the same way, I can imagine someone using "purloined" to hint at a password of PASSWOR. Of course, with only 7 letters that wouldn't work for the comic. You would need a common 9 letter password to make a workable puzzle in the comic, and it's hard to think of anything better than ASDFGHJKL in that context. I appreciate the symmetry of the reference as well, in The Purloined Letter, the trick is that the police are all overthinking things and overlooking the obvious. 108.162.221.16 21:58, 7 November 2013 (UTC)

I don't like "purloined" as a hint for "ASDFGHJK" one bit ("christmas" [that is, "noel"], "eight home", "elephant sneeze with a holiday", or any number of other phrases would be much better if that's what you were trying to clue), but it is the best thing so far. Maybe if we pencil it in, Randall will be motivated to let us know what he *really* meant. (Or apologize for "purloined" being lame.) Cscott (talk) 19:32, 8 November 2013 (UTC)

If there's no objection, I'll go ahead and add this solution to the table above explaining the comic? I don't think there are any other credible candidates. 108.162.218.41 18:50, 12 November 2013 (UTC)

No objection here. I don't like it, but it's the best we've got. Cscott (talk) 15:09, 13 November 2013 (UTC)

Why the restriction on the ending of the Pokemon to el, l, etc? There could be an adjective before (i.e. redkingle), so the Pokemon name could extend more into the second frame. The adjective might be some abbreviated synonym for favorite, or whatever fav (or fay) stand for. 108.162.215.34 22:07, 6 November 2013 (UTC)rbnm

**The last clue**

Regarding it being actually Fay water-3 pokemon, have a look at this: http://www.serebii.net/e-reader/battle/08.shtml

The trainer is named Fay, and has a Starmie, which is a Water-3 Pokemon according to http://bulbapedia.bulbagarden.net/wiki/Water_3_(Egg_Group)

However, its only 7 characters. Not sure if it means anything, but just putting it out there.

EDIT: FayStarmie takes us to 10, leaving 9dca1d79d4dec6d5 meaning 'ie'

EDIT 2: I believe there is a Fay in Pokemon X and Y, but I can't find any information on her. Also Fay could refer to fairy, which is the new type added in Pokemon X and Y, but there doesn't seem to be any fairy Water-3 Pokemon, or any pokemon that reside in both groups. Haelbarde (talk) 00:24, 7 November 2013 (UTC)

It's not "FAY", it's "FAV". Check how "FAVORITE" is written in the middle of the picture, and look at the Y's. The vertex is clearly below the mid-point of A, which is where it is in Y. -199.27.128.119 09:45, 7 November 2013 (UTC)

**Another theory on last part**

Numbers and dates. Other passwords had numbers, why not this one?

A birthday is an easy thing to remember, so it's bound to be someone's password. So lets say a birthday was August 25, 1962. One can write that as august2562, which just so happens to be when Monster Mash was released, as per Wikipedia. In addition, August is quite similar to C. Auguste Dupin, from The Purloined Letter. Lastly, one can add the Pokedex number of the Pokemon to the end of its name, but Poliwrath62 is too long, and is a water 1 Pokemon, not water 3.

This theory doesn't fit perfectly, but I haven't seen it posted yet. Maybe it'll give someone that eureka moment...199.27.128.188 10:11, 7 November 2013 (UTC)

On the "purloined" and "monster mash" things: this is an incomplete theory but might give someone else an idea. Poe's "The Purloined Letter" contains this line: "He is the monstrum horrendum, an unprincipled man of genius." So perhaps the "purloined" clue is a reference to this line somehow. "Monstrum horrendum" is Latin for "horrendous monster" (although in Latin "monster" technically means "something to be pointed out and marvel at"). So if the password is "monsterm", this could be a misspelling of "monstrum"; if it's "monster " it could be a translation, though that begs the question as to why it ends with a space. Darthkiwi (talk) 15:50, 7 November 2013 (UTC)

Could Purloined be a pun for a stolen persistant URL? 199.27.128.113 18:32, 7 November 2013 (UTC)rbnm

I did some copypasting with v's y's and a's in paint and i now know for certain that it's fav pokemon, not fay. Althogh i did think about fay referring to fairy. But i now find this very unlikely. Personally i think it has some relation to water-3 egg group because that is just that obvious to any pokemon player, although it may be some weird distant connection. i usually do a few cryptic things with the password that i can probably remember but makes it as hard as possible to guess. so i might make something like that my hint if my favorite pokemon trainer used a pokemon once who shared the same colors as a water 3 pokemon. so my guess is that it is water-3 but maybe not a pokemon directly in it. 108.162.231.53 18:57, 7 November 2013 (UTC)

I'm wondering if the mash comment could refer to the Mashed Potato dance. From the wikipedia page about said dance, a slightly modified version of it was one of the dances that people danced to the Monster Mash. 108.162.219.35 (talk) (please sign your comments with ~~~~)

---

One technique for creating strong passwords is to take the first letter of each word in a passage from a book/movie quote/song/etc. as seen at http://www.mrsware.com/2/post/2013/06/passwords-revisited.html - "I was working in the lab late one night" would turn into "iwwitllon". If we take the next lyrics from the monster mash after "he did the", we get 'mmhdtmiwags'. The first eight words of The Purloined Letter would spell 'apjadoge'. Not sure how helpful this is.

Another thought is that in the story of The Purloined Letter, the letter is hidden in plain sight. Also, the story starts out with "Nihil sapientiae odiosius acumine nimio" - Nothing is more hateful to wisdom than excessive cleverness, which may be relevant here.

Finally, I was thinking about punctuation. "mon*m#" could be pronounced like "mon-star-m-hash". 199.27.130.146 23:02, 7 November 2013 (UTC)

It's also possible that Monster Mash means combining (mashing) the names of two Pokemon. I believe you guys have only been looking at single pokemon names. Regarding Purloined, could that word be the opposite mashup? So a Pokemon called (I'm making this up, don't hate on me) Purfect and another one named Charloined could mash into Purloined or Charfect. Mirrordude (talk) (please sign your comments with ~~~~)

I don't think that is 'legal' in the rules that everyone is assuming for this game. Note the (simulated) user who picked the pokemon clue is unaware that someone else used monster mash in their clue. This is addressed in more detail above. 173.245.52.158 13:00, 8 November 2013 (UTC)

**Not 1, but 3 Pokemon**

What if the Pokemon clue wasn't a single favorite from the water-3 group, but a favorite group of three water type Pokemon? This is less intuitive from the hint, but do people really pick out favorites from egg groups rather than types? 173.245.54.8 01:41, 8 November 2013 (UTC)

For example, "PokeBroKing" would represent a family of three water Pokemon (Slowpoke, Slowbro, Slowking), and "ING" would be the second hash to use with MonsterMash and the blank hint. 173.245.54.8 03:18, 8 November 2013 (UTC)

**Two Word Monsters?**

What if the most simple derivation summarized above is correct, but with two minor changes:

```
 1) he did the... refers to 'monster' not 'monster mash' since 'mash' appears in the clue (I asked about this above, but nobody commented)
    note that this needs to be a password that you wouldn't guess if you don't also have the purloined clue, so not the word 'monster' or 'monster mash'
itself
 2) assume there is a space making two words in the first 8 characters of the answer to this clue
```

Then the search for 8 character words for 'purloined' would actually be the search for 8 character phrases, like so:

```
purloined -> letter -> 'post man'
monster -> 'post manle' (ok, that's not a monster, but for the correct 'purloined' phrase it would be)
```

This should fix the problem where you can't add short endings to 8 character words and make another word. I think it is easier to add these endings to shorter words. I also like the form of this puzzle, because it would be a logical difficulty progression after the 'Charlie X' thing above. 173.245.52.158 12:52, 8 November 2013 (UTC)

I think you're on the wrong track. The answer for the last one could be "Password|Smash" or "Password|Mash" (rhymes with MonsterMash) capitalization unknown, of course. "OmastarS|mash" or "Omastar |Smash" for the Pokemon. Purloined, of course would be the "Password" itself, self-referential. 108.162.219.23 (talk) (please sign your comments with ~~~~)

**Who did the mash?**

It's right in the lyrics: "my monster". The obvious corresponding answer to the Pokémon clue is to prepend the Pokédex number to the name, eg, "099kingler". It could also be, say, "99 kingler" or "91cloyster", which is unfortunate because we'd prefer a unique solution. Even sadder is that this leaves us with "my monst" for the password with the purloined clue, and that really just makes no sense at all. --108.162.219.38 22:55, 8 November 2013 (UTC)

I might have missed it - did we figure out what the boxes on the right are for? They might be a key to the puzzle. Davheld (talk) 10:57, 10 November 2013 (UTC)

The boxes are just what people have been doing with the fact that each block represents up to 8 characters. You'll notice the rectangles made up of smaller boxes contain 8 boxes. These are only for the passwords which contain two blocks (thus having 9-16 characters). The smaller rectangles not subdivided then tell us that there is 8 or less characters inside it. Haelbarde (talk) 14:05, 11 November 2013 (UTC)

Purrloin is the name of a Pokemon. I would suggest checking Water-3 Pokemon that can breed with Purrloin, but none can. Perhaps another connection? 173.245.54.79 (talk) (please sign your comments with ~~~~)

---

Rob and pick are both synonyms of steal, and the guy who wrote the monster mash is robert pickett. So purloined could be "rob pick" and the other clue just "rob pickett". This doesn't seem to fit with any of the pokemon clues mentioned, but since I know nothing about pokemon mayber there's a way to make it work? -- starwed 108.162.216.19 19:16, 11 November 2013 (UTC)

I like the idea of some permutation of Robert Pickett. I'm sure the ending can be used with some Pokemon, provided the region number is added. What bothers me though is that the answer to monster mash is the same as the one above, which makes me think it should be a common phrase, not a name. But maybe there's a way to mess with Bob's name to turn it into a common phrase. 173.245.54.8 01:18, 13 November 2013 (UTC)

ducklett is a water pokemon belonging to egg group water 1 (so not completely fitting) his pokedex number is 580. disregarding the fact that it's water 1 and not 3 it could be 580ducklett. but even then we don't know for sure if we need a regional or national pokedex number. most pokemon (if not all) appear in more than one pokedex, and they are numbered differently in each one. so it could also be 086ducklett, #86ducklett, 153ducklett, or 127ducklett, along with the aforementioned 580 ducklett. so this would not be unambiguous. and prefixing a pokemon with it's pokedex number means there would be more than one solution to the puzzle. i now think that this is not the correct approach. i also really hope this isn't like a bait and switch, or some other trick to fool us into believing there is a solution, while in fact there is none. 108.162.231.53 22:04, 11 November 2013 (UTC) 173.245.54.39 05:55, 13 November 2013 (UTC)

Hi, the last 4 answers are:

```
monster mash
monster mash
monster
meteor mash
```

thanks for playing --- 173.245.54.39 05:55, 13 November 2013 (UTC)

In your edit summary you say, "it's a move, not a character", and I'm assuming you are referring to Meteor Mash. But how is that a "fav water-3" pokemon (move)? It's *generation 3*, but it's a steel type move. There's nothing 'water' about it. Further, "monster " is still not an acceptable answer for the clue "purloined", and the previous "Charlie " answers have indicated that spaces count. This 'solution' needs more work. Cscott (talk) 15:08, 13 November 2013 (UTC)

EVERY hint and password refers to hackers or hacking [Try googling hacker ___], even possible alternatives such as SHEEN (actor's name) or HARPER (character name). 'Fav of 12 apostles' -- 'hacker 12' reveals news articles about a 12-year old Canadian boy convicted of hacking, and 'hacker apostle' sends you to "The 13th Apostle," an apparently terrible novel about a teenaged hacker.

EVERYTHING is related. 'Apostle' helped us figure out 'weather vane sword' (which was hidden, but a POEm was left hinting at where). '57' seems random - until you PURLOIN 1 from it (I and 1 often interchanged either purposely or accidently) and end up with 56 - and the 56th most common password on the list was asdfghjkl. Eve (talk) 21:24, 13 November 2013 (UTC)

The thought just occured to me that water-3 could refer to the 3rd phase of water, so we might be looking for an ice pokemon instead. Then again, this might just be more noise. 108.162.219.35 (talk) (please sign your comments with ~~~~)

Fav water-3 Pokemon has to be tentacool. It fits the format tentacoo l using the purloined l from asdfghjk l. Tentacool is (was ?) a well-known Pokemon hacker, and tentacool references LaughingSquid and its 'Chief Tentacle' Scott Beale. Finally, tentacool's number is 72, and if you add the numerals in the top half of the passwords (1, 57, 15, 10) and then subtract the numbers-represented by letters in the bottom half of the passwords (x = roman 10 and l = 1) you get 72. Everything is related. Eve (talk) 21:23, 13 November 2013 (UTC)

Eve i have no idea if what your saying is right but either way i think you need to slow down a bit.--Lackadaisical (talk) 23:08, 13 November 2013 (UTC)

Sorry. I'll slow down and back up, and I apologize in advance if this is too much or too verbose. The seeming randomness of both the hints/passwords chosen and their arrangement on the physical page bugged me, especially given the "greatest crossword puzzle" claim. Great crossword puzzles aren't random; they're thematic, amazingly inter-connected, and self-validating. The subject of the puzzle seemed to indicate its theme, so I started googling 'hacker ___,' inserting random words from the hints, and then from the passwords themselves as they were deciphered. The results were kinda amazing and very educational. As I said earlier, everything in the puzzle is related to hackers/hacking, even things you'd think couldn't possibly be. Hacker Sheen, for example, led me to a Sheen News Network story on "Hackers being treated like terrorists," which discussed the Auerheimer and Hammond cases. So, general thematic relevance established, though '57' still bothered me... As did the physical arrangement of the puzzle. Why was 'favorite of 12 apostles' several lines away from "weather vane sword" when these two clues self-validated? Why was 'Judith15' so markedly out of alignment with both of the hints that produced it, which were themselves separated? Questions like these eventually led me to believe that we should look for connections and validations within the puzzle as a whole, not just in consecutive or nearly-consecutive clues. Which brought me back to '57,' and the last group of hints/passwords that seemed to have no connection to any other hints/passwords and no validation within the puzzle...and it finally dawned me that the reason this bugged me so much was that asdfghjkl was the 56th rather than 57th entry in the list of common passwords, and my first thought was Why couldn't it have been 56, and my second thought was But if you take away 1 then it is, and the Eureka moment came when I realized that 'take away' is a synonym of 'purloined' and I and 1 are often interchanged either accidentally or purposefully and 57 - 1 = 56. So then I looked up Tentacool's number, and looked at all the other numbers in the puzzle, to see if they would somehow produce 072. My heart sank when I realized that 1 + 57 + 15 + 10 = 83, and that even subtracting the purloined l/1 didn't get me there, but then I realized that if the x were a roman numeral 10, and it too was subtracted, then the result was 72 and, again, internal validation of an answer. Farfetched? -Sure. Too great a stretch? -Perhaps. Ingenious and beautiful? - Absolutely. Eve (talk) 01:41, 14 November 2013 (UTC)

... I like you --Lackadaisical (talk) 17:49, 14 November 2013 (UTC)

http://nakedsecurity.sophos.com/2013/11/04/anatomy-of-a-password-disaster-adobes-giant-sized-cryptographic-blunder/ points out that the password lengths in the real dump include the null terminator, so that you get one block for 0-7 characters, two for 8-15 and so on. --141.101.98.236 11:41, 19 November 2013 (UTC)

This page was last modified on 31 August 2014, at 15:50.
This page has been accessed 123,953 times.